VOLUME 18 ISSUE 1

KCJIS NEWS

FEBRUARY 2016

OLDER INTERNET EXPLORER VERSIONS SUPPORT ENDS JANUARY 12

DON CATHEY, KCJIS INFORMATION SECURITY OFFICER

Microsoft has announced that security updates and technical support for versions of Internet Explorer older than version 11 will end January 12, 2016. These include Internet Explorer versions 8, 9, and 10. This information has already been disseminated through several administrative messages in OpenFox and service announcements from other technology service providers. More information can be found at: https://www.microsoft.com/en-us/WindowsForBusiness/End-of-IE-support. Excerpts from Microsoft have been provided for further information:

What does End of Support mean?

Staring January 12, 2016, the most current version, Internet Explorer 11, will be available as a fully supported browser. Internet Explorer 11 is the newest version of Internet Explorer, and will continue to receive security updates, compatibility fixes, and technical support on Windows 7 and Windows 8.1.

What does this mean?

After January 12, 2016, Microsoft will no longer provide security updates or technical support for older versions of Internet Explorer. Security updates patch vulnerabilities that may be exploited by malware, helping to keep users and their data safer. Regular security updates help protect computers from malicious attacks, so upgrading and staying current is important.

INSIDE THIS ISSUE

Because Microsoft will no longer support older versions of Internet Explorer, the Kansas Bureau of Investigation's helpdesk will no longer be able to support them either. *As of Tuesday (01/12/2016), the KCJIS network will no longer support any internet explorer version except version 11 as Microsoft will stop posting updates to older browsers after that date. If you are using an internet explorer version older than version 11 make sure to update it before Tuesday to prevent your computer from having issues that could include losing the ability to open KCJIS pages. That includes but is not limited to https://kcjis.ks.gov/ and all pages accessed through it. If you are unsure what version you have check by going to tools>about internet explorer.*

The tools icon looks like this gear: “About Internet Explorer” is also found under Help button on the Menu bar. It is important to note that the only Operating Systems and browser currently supported by the KBI helpdesk are Windows 7 and 8.1 along with Internet Explorer 11. If any browser based application is being used and not provided by the Kansas Criminal Justice Information System (KCJIS), then users must work with the vendor to ensure it will also work with Internet Explorer 11.

Providing support for systems when they break down is important, but protection from vulnerabilities is even more so. The Federal Bureau of Investigation (FBI) Criminal Justice Information System (JCIS) security policy addresses the vulnerability aspect in policy 5.10.4.1 Patch Management. In 2014, Windows XP reached its “End of Life” support, and was deemed out of compliance with the FBI CJIS security policy. It was explained then that when Microsoft, or any other vendor, stops support of products the vulnerabilities can continue to be developed and exploits will still be deployed to take advantage of the lack of support. The same JCIS security policy is being applied now to older versions of Internet Explorer and other software used to access KCJIS regardless of vendor. Compliance to policy 5.10.4.1 is confirmed during Kansas Highway Patrol Information Technology security audits.

INSIDER THREATS

KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP

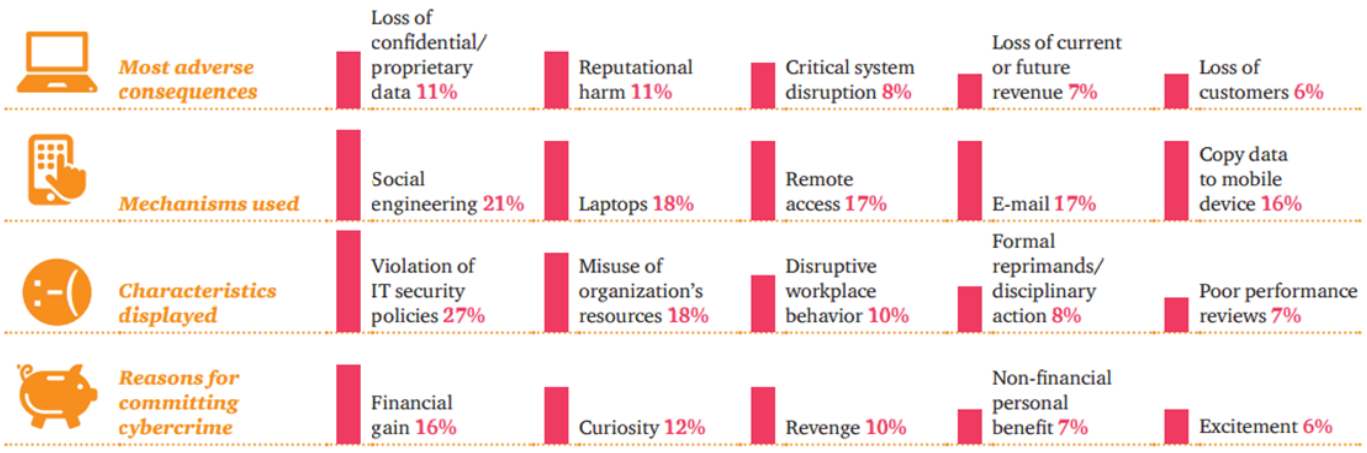
Insider threats are often more costly and damaging than those committed by external threats. Many threats do not treat these internal malicious threats seriously enough or have adequate safeguards (policies, procedures, practice, tools, etc.) to detect or prevent attacks. Whether intentional or unwittingly, insiders engaging in cybercrime act in opposition to the interests of their agencies and the public. Has every agency implemented a plan to deal with internal threats?

Kansas Criminal Justice Information System (KCJIS) Security Policy Area 2 addresses the required Security Awareness topics and training. Yet, agencies can often be apathetic to security training and awareness, dismissing such concerns as a necessary evil, a cost of doing business, or a mandated policy that is enforced only for audit-compliance purposes. In essence, the perceptions of insider risk often do not match reality for many people.

Threats from malicious insiders pose a greater security risk than outsiders. Insiders have a distinct advantage over external actors, because they already have authorized access to internal data and systems. They do not need to breach external security controls that protect network boundaries (firewalls, intrusion prevention systems, etc.). These insider threats can include personnel who want to steal or leak confidential or protected information, commit sabotage, or other malicious acts (i.e., monetizing information for financial gain or an aggrieved employee seeking retaliation after feeling unfairly passed over for promotion).

A malicious insider threat is defined as a current or former employee or private contractor who has had authorized access to an organization's network, system, or data, and intentionally misuses that access to negatively affect confidentiality, integrity, or availability of the organization's data or information systems. Figure 1 (below) lists the causes and consequences of cybercrime committed by insiders.

Figure 1: The causes and consequences of cybercrime committed by insiders*



*A current or former employee, service provider, authorized user of internal systems, or contractor

Source: 2014 US State of Cybercrime Survey, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

Insider threats are not always malicious in nature. Information breaches can also occur through negligence or misuse of systems. Outside adversaries do not need to breach external network security system boundaries if they can obtain access from an agency employee – preferably someone with administrative privileges. Getting an employee to click on a link or pop-up window or opening a common file attachment, such as a PDF or JPG file, can allow an adversary to install a backdoor tunnel into the information system or to install malicious software, such as keyloggers and screen capture programs.

Insiders can be motivated by financial gain, retribution, or for other reasons. They can also simply be ignorant or careless when it comes to practicing secure security measures. People can pose real threats to agencies, such as Criminal Justice Information (CJI),

INSIDER THREATS (CONTINUED)
KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP

when they gain unauthorized access, disclose confidential data without authorization, or when they sabotage an organization's systems, network, or data. These people can be a real danger and must be taken seriously.

Security controls should be configured on all network devices where possible. User permissions and access should be limited to the level necessary to perform their job duties. Regular reviews of agency user accounts and associated permissions (especially those with administrative privileges) will help to mitigate risk to information systems and internal data. Refer to KCJIS Security Policy Area 5.5 for specific policy requirements in the sections on User Account Review and Access Control. Have plans implemented to deal with internal threats? If not, start today!

AMY JOHNSON, KHP CJIS UNIT
KCJIS CONFERENCE COMMITTEE

SAVE THE DATE

16TH ANNUAL KCJIS CONFERENCE

JUNE 5-7, 2016 Hutchison, KS

The KCJIS conference will feature vendors and a number of presenters with beneficial information for those criminal justice personnel that work with CJIS and KCJIS systems.

A Few Topics Featured This Year:

Open Records
PSAP Interoperability
Radicalization- Local Terrorism
Situation Awareness
Sex Offender Process
Violent Person
FBI Security Policy V5.4 & V5.5
Cloud Security & Virtualization
Security Threats
Open Fox
NLETS

Presentations by:
FBI CJIS Unit, FBI CJIS ISO Unit, Homeland Security, Attorney General, Kansas Ofc Of Emergency Communication, KHP, & KBI

The conference schedule will soon be available. Once completed, conference information can be found on your agency terminal through administrative messages, the KCJIS Web Page, or the CJIS Launch Pad https://cjisaudit.khp.ks.gov/launchpad/

KANSAS OFFENDER REGISTRATION ACT QUESTIONS & ANSWERS

JENNIFER SLAGLE, PROGRAM CONSULTANT KBI

Are certain parts of the Kansas Offender Registration Act (KORA) confusing? The Kansas Bureau of Investigation (KBI) is here to help! These are some frequent questions and answers to help clarify several important points regarding KORA:

Does an offender need to report volunteer work?

"[E]mployment means any full-time, part-time, transient, day-labor employment or volunteer work, with or without compensation…" K.S.A. 22-4902(i). Yes, if the volunteer work meets the criteria of three or more consecutive days or parts of days or ten nonconsecutive days over a period of thirty consecutive days.

What vehicles need to be reported by an offender?

"[A]ll vehicle information, including the license plate number, registration number of and any other identifier and description of any vehicle owned or operated by the offender, or any vehicle the offender regularly drives, either for personal use or in the course of employment, and information concerning the location or locations such vehicle or vehicles are habitually parked or otherwise kept." K.S.A. 22-4907 (a)(12).

Any personal vehicle that the offender owns, operates, or drives on a regular basis should be reported. This also includes vehicles owned by someone else such as a car owned by a parent, spouse, friend, etc. that the offender regularly drives. Work vehicles must also be registered.

When does an offender have to pay the registration fee?

"[R]emit payment to the sheriff's office in the amount of $20 as part of the reporting process…in each county in which the offender resides, maintains employment or is attending school. Registration will be completed regardless of whether or not the offender remits payment" K.S.A. 22-4905 (k). Fee payment is not required:

1. "when an offender provides updates or changes in information or during an initial registration…" K.S.A. 22-4905 (k)(1)
2. "when an offender is transient and required to register every 30 days…" K.S.A. 22-4905(k)(2)
3. "if an offender has, prior to the required reporting and within the last three years, been determined to be indigent by a court of law…" K.S.A. 22-4905 (k)(3)

An offender is required to pay twenty dollars during his or her birthday month as well as every third, sixth, and ninth month thereafter. Offenders are not required to pay the twenty dollar fee if they are updating information during a month where they are not required to report. Transient offenders are only required to pay during their four required reporting months. If an offender is found indigent by the court, it can only be applied to offender registration fees and is valid for three years.

What can the registration fees be used for?

"All funds retained…shall be credited to a special fund of the registering law enforcement agency which shall be used solely for law enforcement and criminal prosecution purposes…" K.S.A. 22-4904 (d)(9)

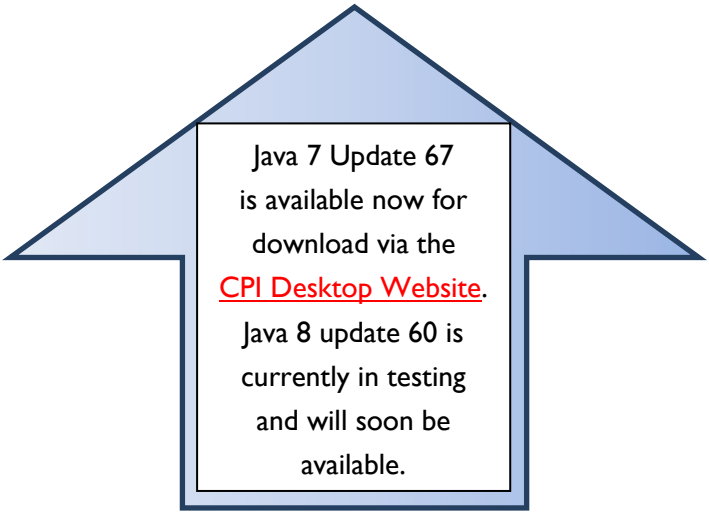
If someone gets their conviction expunged, do they still have to register?

"…[W]hen a court orders expungement of a conviction or adjudication that required an offender to register pursuant to the KORA, the registration requirement for such conviction or adjudication does not terminate. Such offender shall be required to continue registering pursuant to the KORA, but shall not be subject to public registration" K.S.A. 22-4910 €. Yes, they will have to continue to register, but their record will be restricted and not accessible by the public. If someone searches the public website, then the offender will not be listed. If there are additional questions, please contact the KBI Offender Registration Unit at (785) 296-2841.

NEWS FROM THE KBI HELP DESK
JAVIER BARAJAS, NETWORK CONTROL TECHNICIAN KBI

10-day Grace Period for Online Vehicle Tag Renewals

As a reminder, Kansas Department of Motor Vehicles (DMV) implemented a 10-day renewal grace period that starts the day of the tag's expiration date as of July 1, 2015. Vehicle tags can be renewed online at KSWebTags.org on the last day of the month without being ticketed for expired registration. The online renewal paid receipt may be printed and kept in the vehicle or stored on the owner's mobile device until the decal arrives. Either will serve as proof of compliance that the vehicle owner was registered on time to law enforcement. This grace period does not apply by statute if the electronic renewal was completed after the violation or if the renewal was completed at any time by mail or in person. It also does not apply to fleet tags or commercial trucks registered over ten thousand pounds.



Accuvant and FishNet Security Become Optiv Security

Accuvant and FishNet Security merged in early 2015. On Aug. 5, 2015, they announced that their merger had finished, and have launched their new brand name: Optiv Security. For more information about Optiv Security, visit their website at www.optiv.com. Please send all requests or correspondence to the Optiv Security Purchasing Department at tokens@optiv.com.

Entering Stolen Decal Sticker

When entering a stolen decal sticker, use the Enter Article - EA message key. Use the code 'JSTICKE' in the Type field, 'DECAL' in the Brand field, and the decal number (which should be the same as the plate number) in the SER field. Finally, indicate that this is a stolen decal sticker from a vehicle plate in the Miscellaneous Information field.

Internet Explorer Version 11

As of 1/12/2016, Microsoft will no longer support Internet Explorer versions 8, 9, and 10. As the Kansas Bureau of Investigation's (KBI) Help Desk will no longer support older versions, it is recommended that all Kansas Criminal Justice Information System (KCJIS) agencies update to Internet Explorer 11.

Decommission of TRS Link on KCJIS Web Portal

What happened to the TRS Link on the KCJIS Web Portal? The legacy portal TRS search link has been marked for removal. When the new KCJIS Portal, https://kcjis.ks.gov/my.policy deployed, the old link and legacy portal application were removed. KCJIS users can access traffic records by conducting a Master Search on the KCJIS Web Portal and then selecting 'CRASH' for the data source.

Non-Conforming VIN for NCIC Supplemental Sex Offender file.

The supplemental message key for the National Crime Information Center (NCIC) sex offender file does not contain a miscellaneous field; however, a non-conforming Vehicle Information Number (VIN) in a NCIC record does require the miscellaneous field. NCIC does allow for a non-conforming VIN to be added via the supplemental message key to be added on the Sex Offender file. The base record must first contain "SVIN" at the beginning of the miscellaneous field. Once the miscellaneous field starts with SVIN in the base record, single or multiple non-conforming VINs will be added to the supplemental record. The supplemental message key will accept non-conforming VINs in the VIN field only if the miscellaneous field in the base record starts with SVIN.

KCJIS User Group

Ginny Eardley of the Kansas Bureau of Investigation's Information Services Division provided information on Expungements at the January meeting. The next KCJIS meeting will be March 3rd, 2016 at 12:00 PM in the Auditorium of the KBI Headquarters building in Topeka, Kansas.

KANSAS BUREAU OF INVESTIGATION MARCH TRAINING
LESLIE MOORE, ISD DIRECTOR KBI

March 8th and 9th at KBI Headquarters:

- Criminal History – Electronic Dispositions
- Ident – Fingerprinting and Palm Printing Requirements
- Incident Based Reporting Requirements
- Rapsheet Differences – KCJIS vs III
- Central Message Switch
- Offender Registration Requirements
- KsORT

For additional information, please go to the calendar on the KCJIS web portal at https://kcjis.ks.gov. Class times and sign up instructions are located on the calendar.

The KCJIS Newsletter is published by the
Kansas Criminal Justice Coordinating Council

KANSAS BUREAU OF INVESTIGATION

Alicia Madison
Newsletter Editor
1620 SW Tyler
Topeka, KS 66612
785-296-3302
Alicia.Madison@kbi.state.ks.us